Service Oriented Computing and Applications (2022) 16:143–145
https://doi.org/10.1007/s11761-022-00348-2

EDITORIAL NOTES

The process of risk management needs to evolve with the changing technology in the digital world

Omar Khadeer Hussain[1]

Published online: 12 August 2022

1 How has the digital world's evolving landscape changed the risk management process?

Risk and its management play a critical role in the success of any business or computing activity. To a decision-maker, it assists in making informed decisions while simultaneously managing the impact of events that may lead to failure. Due to its importance, risk management has been applied in different domains that range from health [1], business [2], engineering [3] and computing [4]. Despite its importance, as with any field, the risk management process must constantly evolve to best achieve its aims. This requires the risk management process to become interdisciplinary in nature to reap the benefits of other technologies in pursuing its objectives. Recent advancements such as Big Data, Data Analytics and Blockchains have enormously benefitted different domains in achieving their aims more effectively and efficiently. The field of risk management is no exception to these advancements and has benefitted widely too in domains such as insurance [5], supply chain management [6], marketing [7] and customer churn reduction [8]. Using these initiatives, companies have tailored their risk management practices to best achieve their strategic outcomes. A report by EY states that such a shift in risk management from focusing on subjective and individual perception to one that focuses on dealing with the constantly changing landscape is termed Risk Enabled Performance Management (REPM) [9]. REPM takes a proactive approach to manage risks by identifying beforehand the risk trends and factors before managing them to achieve the goals. Artificial intelligence (AI) techniques have played and will continue to play a significant role in achieving REPM aims.

✉ Omar Khadeer Hussain
o.hussain@adfa.edu.au

[1] School of Business, UNSW Canberra, Canberra, Australia

2 Open issues

However, with the ever-increasing data and use of analytics and AI for proactive risk management, there needs to be a fine line of divide between complete automation and moderation by a domain expert in risk management [10]. This is supported by research involving 1500 companies that state those who depend entirely on their automated AI processes see short-term gains [11]. On the other hand, if humans and machines work together, significant performance improvements are experienced. In the domain of risk management, the following open issues need to be addressed to realize the aim of humans and machines working together:

2.1 Explain the results apart from just presenting them

Besides giving an output, machines should explain to humans why that output is given. In a quest to improve the performance of prediction results, AI models have become opaque in their working nature [12]. This leaves humans with no chance of influencing the inputs of the model. To address this, a new area of research, eXplainable AI (XAI), is worked on in the literature. XAI emphasizes the need for AI techniques to explain their black box-based outputs to humans so they can be interpreted and trusted [13]. This is needed, especially in the enterprise domain, where incorrect solutions can lead to severe consequences [14]. Novel XAI methods such as SHAP (SHapley Additive exPlanations) [15], LIME (Local Interpretable Model-agnostic Explanations) [16], LINDA-BN (Local Interpretation-Driven Abstract Bayesian Network) [17] assist in interpreting the decision output and build trust in it. However, a common shortcoming of these approaches is that they do not capture and model the interdependencies among the decision features. As a result, from the perspective of risk management, they cannot measure how changing a single feature in a time affects the decision output in another period. This is particularly important in an interconnected

system, where a feature is dependent or impacted by many others, influencing the quantified risk.

2.2 Real-time identification of risk events for their timely management

Apart from just identifying risks, the risk management process must do that on time. If not, the benefits of proactive risk management may not be realized. Researchers have used AI techniques such as reinforcement learning (RL) to achieve this aim [18]. In a dynamic environment, this benefits humans as they do not have to provide different types of training data. Instead, it utilizes the ability of the RL model to explore and present to humans what it thinks might be beneficial in the scheme of things [18]. Furthermore, this also gives confidence to the humans that the developed model not only replicates what it is trained on but also adapts to the changing environment based on human feedback. However, to assist the RL-based model in correctly identifying only those events related to the risk event of interest, human input is needed. This may be in different forms, such as a knowledge graph that links different events according to a similarity measure or the ability to process and link different events, leading to the occurrence of the risk event of interest (Complex Event Processing) [19]. These will give the RL-based model to traverse a path in its quest to recommend relevant results that make sense and are of use.

2.3 Validating the authenticity of subjective information for blockchain processing

In Blockchains, a transaction is made directly without any trusted third parties. The consensus among blockchain participants needs to be achieved by mechanisms such as Proof of Capacity (PoC), Proof of Work (PoW) or Proof of Authority (PoA) before transactions become a part of the blockchain. While achieving such consensus on transactions, blockchain participants must verify the authenticity or truthfulness of the information contained within those transactions. Verifying the authenticity or truthfulness of the transaction's information is easy if it comes from an *objective* source. An objective source is one where the information's originating source has a digital footprint, and thus, its authenticity can be verified and validated by publicly available documents, transactions or reputation. This is not present for information from a *subjective* (or non-objective) source, for example, a personal opinion or a claim [20]. Thus, verifying its truthfulness and authenticity is not as straightforward as it is for objective information. While subjective information may not be prevalent in domains where Blockchains are commonly used, such as cybersecurity [21] and healthcare information sharing [22], they are present in domains such as Supply Chain Risk Management (SCRM), the art industry, real estate, blood supply chains, etc. Thus, the authenticity of such information needs to be verified before Blockchains can be effectively used for risk management in such domains. Without this, the current applications of Blockchains in such domain are limited to tracking of information [23], checking the provenance of products [24], etc.

References

1. https://catalyst.nejm.org/doi/full/ https://doi.org/10.1056/CAT.18.0197.
2. https://www.investopedia.com/articles/financial-theory/09/risk-management-business.asp.
3. https://www.mitre.org/publications/systems-engineering-guide/acquisition-systems-engineering/risk-management.
4. https://securityscorecard.com/blog/what-is-information-risk-management.
5. https://www.mckinsey.com/industries/financial-services/our-insights/how-data-and-analytics-are-redefining-excellence-in-p-and-c-underwriting.
6. https://www.everstream.ai/articles/using-supply-chain-predictive-analytics-to-reduce-risk/.
7. https://knowledge.wharton.upenn.edu/article/marketing-future-data-analytics-changing/.
8. https://mixpanel.com/blog/churn-analytics/.
9. https://www.ey.com/en_in/risk/role-of-data-analytics-in-risk-management.
10. https://www.forbes.com/sites/forbestechcouncil/2019/10/30/why-ai-needs-human-input-and-always-will/?sh=751f3bcb5ff7.
11. https://hbr.org/2018/07/collaborative-intelligence-humans-and-ai-are-joining-forces.
12. Boge FJ (2021) Two dimensions of opacity and the deep learning predicament. Minds Mach 32(1):43–75. https://doi.org/10.1007/s11023-021-09569-4
13. Dhanorkar S, Wolf CT, Qian K, Xu A, Popa L, Li Y (2021) Who needs to know what, when?: Broadening the Explainable AI (XAI) Design Space by Looking at Explanations Across the AI Lifecycle. In: presented at the designing interactive systems conference 2021, Virtual Event, USA, 2021. Available: https://doi.org/10.1145/3461778.3462131
14. Liao QV, Gruen D, Miller S (2020) Questioning the AI: informing design practices for explainable ai user experiences. In: Proceedings of the 2020 CHI Conference on Human Factors in Computing Systems: Association for Computing Machinery, 2020, pp 1–15
15. Lundberg SM, Lee SI (2017) A unified approach to interpreting model predictions. In: presented at the proceedings of the 31st international conference on neural information processing systems, long beach, California, USA
16. Visani G, Bagli E, Chesani F, Poluzzi A, Capuzzo D (2021) Statistical stability indices for LIME: obtaining reliable explanations for machine learning models. J Op Res Soc 73(1):91–101. https://doi.org/10.1080/01605682.2020.1865846
17. Moreira C, Chou Y-L, Velmurugan M, Ouyang C, Sindhgatta R, Bruza P (2021) LINDA-BN: An interpretable probabilistic approach for demystifying black-box predictive models. Decis Support Syst 150:113561
18. Aboutorab H, Hussain OK, Saberi M, Hussain FK (2022) A reinforcement learning-based framework for disruption risk identification in supply chains. Future Gener Comput Syst 126:110–122. https://doi.org/10.1016/j.future.2021.08.004

19. Nawaz F, Hussain O, Hussain FK, Janjua NK, Saberi M, Chang E (2019) Proactive management of SLA violations by capturing relevant external events in a Cloud of Things environment. Future Gener Comput Syst 95:26–44. https://doi.org/10.1016/j.future.2018.12.034
20. Bui HT, Hussain OK, Prior D, Hussain FK, Saberi M (2022) Proof by Earnestness (PoE) to determine the authenticity of subjective information in blockchains - application in supply chain risk management. Knowl-Based Syst 250:108972
21. Taylor PJ, Dargahi T, Dehghantanha A, Parizi RM, Choo K-KR (2019) A systematic literature review of blockchain cyber security. Digit Commun Netw 6(2):147–56
22. Leeming G, Cunningham J, Ainsworth J (2019) A ledger of me: personalizing healthcare using blockchain technology. Front Med. https://doi.org/10.3389/fmed.2019.00171
23. https://www2.deloitte.com/us/en/pages/operations/articles/blockchain-supply-chain-innovation.html.
24. https://www.provenanceproof.com/provenance-proof-blockchain.